

RECEIVED

AUG 11 1997

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20544

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
Implementation of the)
Communications Assistance)
for Law Enforcement Act)

DOCKET FILE COPY ORIGINAL

**COMMENTS ON PETITION FOR RULEMAKING
OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY
AND THE ELECTRONIC FRONTIER FOUNDATION
(RESPONSE TO JULY 16, 1997 PETITION OF THE CELLULAR
TELECOMMUNICATIONS INDUSTRY ASSOCIATION)**

The undersigned privacy organizations urge the Commission to institute a rulemaking proceeding to protect the privacy interests of the American public as the telecommunications industry and law enforcement proceed to implement CALEA,¹ the "digital telephony" law.

Under pressure from the Federal Bureau of Investigation (FBI), the industry has drafted a CALEA implementation standard that would require wireless telephone companies to turn their customers' phones into location tracking devices.

Furthermore, in a decision that has potentially far-reaching implications for the future of telephony, the Internet, and government surveillance, the proposed standard presumes and appears to require that telecommunications companies using "packet switching" provide the full content of customer communications to the government even when the government is only authorized to intercept addressing or signaling data. Thereby, the standard fails to satisfy the

¹ Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414 (1994) (codified at 47 U.S.C. 1001 et seq.).

privacy protections of the wiretap laws and fails to meet CALEA's requirement to "protect the privacy and security of communications ... not authorized to be intercepted." CALEA § 103(a)(4), 47 U.S.C. 1002(a)(4).

In light of these serious threats to privacy, we urge the Commission to:

- (1) adopt a CALEA implementation standard that deletes these location tracking and packet switching features from the proposed industry standard;
- (2) require industry and law enforcement to develop an additional standard for packet switching that affirmatively protects the privacy of content information that law enforcement is not authorized to receive; and
- (3) reject any requests by the FBI or other agencies to further expand the surveillance features proposed in the draft industry standard.

The intent of Congress in adopting CALEA was to preserve, but not expand, government surveillance capabilities. Moreover, CALEA imposes on telecommunications carriers an affirmative obligation to "protect the privacy and security of communications ... not authorized to be intercepted." The statute grants to the Commission authority to oversee CALEA implementation, and, if necessary, to adopt standards for implementing the law in a balanced manner. We are urging the Commission to exercise its authority under the statute to ensure that implementation is carried out in a manner that protects privacy and does not expand government surveillance capabilities.

-- *Parties to this Petition*

The Center for Democracy and Technology (CDT) is an independent, non-profit, public interest organization in Washington, D.C., working to develop and implement public policies to protect and advance privacy and other democratic values in the new digital communications media. The Electronic Frontier Foundation (EFF) is a non-profit public interest organization devoted to protecting civil liberties and promoting responsibility in digital media.

CDT and EFF may have divergent views on CALEA. If the Commission initiates a proceeding, our organizations may have divergent views on specific implementation issues. But we agree that implementation of CALEA raises serious privacy issues that have not been adequately addressed by industry and law enforcement, and that it is the role of the Commission to address those issues.

I. The Commission Must Intervene Now in the CALEA Process Because Industry and Law Enforcement Have Failed to Develop a Standard that Protects Communications Privacy as Required by the Statute

CALEA imposes on the telecommunications industry four requirements. Three of these requirements are intended to preserve law enforcement's surveillance capabilities, but the fourth also mandates protection of privacy. Carriers are required to ensure that their systems are capable of (1) expeditiously isolating and enabling law enforcement to intercept call content; (2) expeditiously isolating and enabling the government to access "call-identifying information," a defined term; (3) delivering intercepted communications and call-identifying information to the

government in a format that allows it to be transmitted to a law enforcement listening plant; and (4) doing so "in a manner that protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted" and the confidentiality of the interception. CALEA § 103(a)(1) - (4), 47 U.S.C. 1002(a)(1) - (4) (emphasis added).

-- The FBI Has Attempted to Dominate the CALEA Standards Process, in Contravention of Congress' Clear Intent

In adopting CALEA, Congress made it clear that the FBI and the Justice Department were not authorized to dictate the design of telecommunications networks.² Instead, CALEA deferred in the first instance to industry bodies to set technical standards to implement the broad requirements of section 103. CALEA section 107, 47 U.S.C. 1006. The telecommunications industry has developed a proposed standard to implement these requirements. TIA/EIA Standards Proposal No. 3580, "Lawfully Authorized Electronic Surveillance." The FBI and other law enforcement agencies had extensive involvement in this process -- involvement that we believe went well beyond the "consultation" contemplated by CALEA and amounted to an attempt to dominate the process. Industry rewrote its standard in many respects to accommodate the FBI's positions. As a result of these concessions, the proposed industry standard already goes too far in enhancing the surveillance powers of the government and fails to

² Section 103(b)(1) of CALEA provides, "This title does not authorize any law enforcement agency or officer -- (A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service" 47 U.S.C. 1002(b)(1).

protect the privacy and security of communications not authorized to be intercepted, and therefore violates CALEA.

However, according to the petition filed by the Cellular Telecommunications Industry Association (CTIA), the FBI and some other law enforcement agencies were not satisfied with the many concessions they received from industry. The FBI and these other law enforcement agencies have blocked adoption of industry's proposed standard, claiming that the industry proposal does not include certain capabilities, sometimes referred to as the "punch-list," which the objectors claim are mandated by CALEA.

II. The Proposed Industry Standard Already Goes Too Far in Enhancing Location Tracking And Failing to Protect the Privacy of Packet Switched Communications That Government is Not Authorized to Intercept

On July 16, CTIA petitioned the Commission to institute a rulemaking and adopt the proposed industry standard. We believe that the Commission ought to act now to adopt this standard, with modifications noted below to address those portions which violate the privacy and security requirements of CALEA. Had CTIA not filed, and barring industry acquiescence to the FBI's recommendations, it was widely expected that the FBI would have petitioned the Commission to impose a standard that included all of the FBI's demands.

The question posed by the CTIA petition is simple: Is there any support in the language of CALEA or the legislative history for the FBI's claim that a CALEA standard must include the additional surveillance features on the FBI's "punch-list?" We believe that the answer to this is clear:

there is no evidence that Congress intended to mandate the specific additional capabilities over which the FBI blocked adoption of the standard. Since it is clear that Congress intended to defer to industry, and since there is no evidence that Congress intended to mandate the specific features sought by the FBI, the Commission has no authority to adopt a standard that adds additional provisions sought by the FBI and other law enforcement agencies.

A. The Proposed Industry Standard Fails to Protect Privacy and Violates the Statutory Privacy and Security Requirements of CALEA

However, there is a separate issue, not raised by the CTIA petition, which is within the Commission's jurisdiction: Does the proposed industry standard go too far in expanding law enforcement surveillance capability and allowing carriers to disclose the content of communications when the government is not authorized to receive content, thereby failing to satisfy the privacy requirement of section 103(a)(4)? It is this issue that we urge the Commission to consider. As we explain below, we believe that industry's proposed standard is deficient for expanding surveillance capabilities and for failing to protect the privacy and security of communications not authorized to be intercepted.

At least two provisions of the industry proposed standard already violate CALEA:

- Location - The proposed industry standard requires cellular and PCS carriers to provide law enforcement agencies with location information at the beginning and end of any

cellular and PCS communication. Attachment A consists of sections 5.4.5 (Origination) and 5.4.8 (Release) of the draft standard. It was the express intent of Congress, supported by the Director of the FBI on the record in public testimony, that CALEA not include any requirement to provide location or tracking information.

At the Joint House and Senate hearings leading to enactment of CALEA, FBI Director Freeh expressly testified that CALEA would not require carriers to make location information uniformly available. Director Freeh testified that "call setup information" (later changed to "call-identifying information") as a CALEA requirement was not intended to include location information. Freeh was very clear in disavowing any interest in covering such information:

"[Call setup information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called 'tracking' information."

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2d Sess. 6 (1994).

Indeed, the industry standard concedes this point when it defines "call-identifying information" in a way that does not include location information.³

- Packet Data Content Delivery - In the future, telecommunications systems will rely increasingly on "packet switching" technologies, such as ATM ("Asynchronous Transfer Mode"), similar to those used on the Internet. This development has potentially profound implications for government surveillance. In a packet switching system, communications are broken up into individual packets, each of which contains addressing information that routes the packets to their intended destination, where they are reassembled. Previously utilized primarily on the Internet for electronic communications, this technology offers substantial advantages in the voice environment as well, and telecommunications companies are beginning to incorporate it in their systems.

On the apparently untested assumption that it is not feasible to provide signaling information separate from the content in a packet switching environment, industry's proposed standard allows companies to deliver the entire packet data stream -- including call communications -- when law enforcement is entitled to receive only dialing or signaling information under a so-called pen register order.⁴

³ The location issues raised here are very different from those previously considered by the Commission in its proceeding on E911 services. In the 911 context, the caller presumptively consents to being located when he or she calls 911. However, other wireless callers do not give consent to be located, so the provision of this information does pose privacy issues.

⁴ There is no provision in the standard that states that companies must provide all packets when the government is authorized to receive

Such orders are issued without probable cause and without the discretionary review accorded to full call content interceptions. The proposed CALEA standard relies on law enforcement to sort out the addressing information from the content, keeping the former but ignoring the latter. This violates section 103(a)(4)(A) of CALEA, which requires carriers to ensure that their systems "protect[]the privacy and security of communications and call-identifying data not authorized to be intercepted."

This approach, were it followed, could well represent a total obliteration of the distinction between call content and signaling information that was a core assumption of the Electronic Communications Privacy Act and of CALEA itself. In the old analog systems, law enforcement agencies authorized to receive signaling information were provided with access to the target's entire telephone line, including content. With subsequent developments in technology, the signaling data was carried on a channel separate from the call content. In this respect, technology itself enhanced privacy, creating an environment in which a law enforcement agency conducting a pen register would receive only so much as it was entitled to receive, and no more. Absent CALEA, packet switching might have undone that privacy enhancement. But CALEA imposed on the telecommunications industry an affirmative obligation to protect communications not

only signaling information. Rather, the standard is deficient because it allows carriers to deliver packets over the signaling channel and fails to require the separation of addressing information from content. See sections 4.5.2 and 5.4.6 of the standard, attachment B. It is our understanding that this issue was raised and debated in the drafting of the standard and that industry and the FBI understood that carriers

authorized to be intercepted. The proposed industry standard has failed to do this. In the proposed standard, industry and FBI have tacitly agreed not to try to ensure that law enforcement agencies get only the information appropriate to the level of authorization in hand.

Accordingly, we recommend that the Commission (1) delete any treatment of packet switching from the initial CALEA standard that we urge the Commission to adopt at this time and (2) direct industry and the FBI to institute a separate standards proceeding to examine the privacy and security aspects of packet switching and determine whether, and if so how, call content can be withheld from the government when the government is not authorized to receive it.

Before casting aside a basic assumption of the wiretap laws, there should be a careful technical examination of whether call-identifying information can reasonably be separated from the full data packet. Otherwise, Congress may have to act to make it clear that the government can access packet data information only in response to a Title III order, not in response to a pen register order.

B. The Additional Surveillance Enhancements Sought by the FBI Have No Support in the Text or Legislative History of CALEA and Would Further Render the Standard Deficient

At least in the foregoing respects, and perhaps in others, the standard already exceeds the outer limits of what Congress intended to mandate through CALEA. The FBI, however, has made it clear that it is not satisfied with the

would be providing all packets to the government and relying on the

standard. The FBI urged expansion of the standard to require functionality that goes even further beyond anything Congress contemplated. If the FBI's demands were accepted, the standard would be rendered further non-compliant with section 103(a)(4)(A).

The following "punch-list" items are of specific concern:

- Multi-party monitoring - Law enforcement proposes in FBI Comment 43 an overly-expansive reading of both the electronic surveillance laws and CALEA, requiring monitoring of all parties to a multi-party (conference) call even after the legally designated subject of the intercept order is no longer participating in the call. The purpose of CALEA was to maintain surveillance of the target in new telecommunications environments, not to facilitate monitoring of those left behind after the subject of the court order is no longer on the call. Law enforcement specifically seeks to monitor the held portion of a conference call even when it is known that the subject is on another call entirely. Not only is this not mandated by CALEA, but providing it would violate section 103(a)(4)(A), since law enforcement is not authorized to intercept the calls of people not named in the order when they are not using the facilities named in the order.

- Expanded definition of call-identifying information - The FBI/law enforcement objections to the proposed industry standard seek an expanded definition of "call-identifying information." The FBI has argued that the standard should

government to sort out the addressing information from the content.

provide the following information, which cannot be characterized as "call-identifying:"

(a) In-band digits that the subject dials after cut-through. These digits do not identify a call in any sense but rather are content-related. Because Congress was specifically concerned with maintaining the distinction between call-identifying data and call content, it included in CALEA an amendment to the pen register statute to require law enforcement when executing a pen register to use equipment "that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." CALEA section 207(b), codified at 18 U.S.C. 3121(c). Furthermore, the legislative history for CALEA states, "Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." H.R. Rep. 103-827, Part 1, at 21.

(b) Notification when the subject is signaled by the subject's services (e.g., message waiting indicator). This network intelligence does not identify a call and is outside the scope of CALEA.

(c) Party hold, drop, and join messages to indicate the status of parties to a call. These messages do not relate to call-identifying information but rather seek to enhance law enforcement investigative techniques beyond the status quo.

(d) "Flash hooks and feature key usage." The FBI wants companies to include on the data or call-identifying channel

these other elements of information, which do not fit within the definition of "call-identifying information" in CALEA.

- Pen Register Information - By the foregoing changes, the FBI is seeking to increase the amount of information that it obtains under the minimal standard applicable to pen registers. But to the extent technologically possible, pen register information should be limited to the express requirements of the pen register statute - "electronic or other impulses which identify the numbers dialed or otherwise transmitted." 18 U.S.C. 3127(3). This simple phrasing in the pen register statute dovetails completely with CALEA's definition and the definition of call-identifying information in the industry-proposed standard. Other signaling or sounds that do not relate to dialed numbers are neither encompassed by the pen register law nor required by CALEA. Currently, law enforcement receives information through pen registers (or the more sophisticated "dialed number recorders") that is outside the pen register statute. The fact that hook flashes, for example, are recorded today does not mean that the pen register statute or CALEA mandate that they be reported in a digital environment in response to a pen register order. Indeed, if the technology allows them to be filtered out, CALEA requires that they not be provided to the government, for they are not authorized to be intercepted.

- Feature Status Message - The FBI seeks to insert a feature status message that would be activated whenever a subject's services are changed by a carrier in response to a

routine administrative request or otherwise. A subject may request a change of services by mail or with a call from a facility not under authorized surveillance. Requiring the carrier to send a message to law enforcement on the target's line whenever services are altered in response to a customer request would require companies to digitize customer information and make it available over the data channel. This would be a significant precedent -- requiring carriers to generate a type of on-line customer service profile solely for the benefit of government surveillance. This information currently is provided by subpoena and can continue to be provided in that manner. There is no basis in CALEA for requiring telecommunications carriers to add this information to their signaling channels.

III. Expeditious Commission Oversight of CALEA Implementation is Essential in Order to Fulfill the Goals of CALEA

The Commission should act upon this petition for two reasons: (1) The voluntary standards setting process contemplated by Congress has not worked because the FBI and other law enforcement agencies used the standards balloting process to block adoption of a standard. (2) Even the draft industry standard goes beyond the intent of Congress and fails to satisfy the privacy mandate of CALEA.

If the Commission does not act, CALEA will take effect in a little more than a year from now (October 25, 1998) in an atmosphere of uncertainty that reduces the chances the statute will be enforced in the balanced manner intended by Congress. At that time, the FBI will be able to bring an enforcement action against a carrier, using the industry-

proposed standard as a floor and the FBI's additional proposals as a ceiling.

Congress clearly intended the Commission to have a role in overseeing, and if necessary deciding, the privacy and security issues posed by CALEA. Section 107 of CALEA explicitly states:

"If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical or requirements or standards that ...

(2) protect the privacy and security of communications not authorized to be intercepted;"

47 U.S.C. 1006. This role for the Commission was obviously an important part of the structure that Congress intended to create in adopting CALEA. The report of the House Judiciary Committee on CALEA states:

"H.R. 4922 includes provisions, which the FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill --
...

4. Allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements, and provides that one factor for judging those standards is whether they protect the privacy of communications not authorized to be intercepted."

H.R. Rep 103-827, Part 1, 17-18. This oversight of the standards process is well within the competency of the Commission. At a hearing on the CALEA legislation, the deputy chief of the Common Carrier Bureau testified:

"Two of the duties that the legislation would assign to the Commission concern the establishment of technical standards and the resolution of disputes ... with respect to reimbursement for costs

"The role assigned to the Commission in these areas is consistent with responsibilities that the Commission has exercised in the past in analogous areas. In particular, the standards-setting process contemplated by the legislation is designed to rely principally on industry efforts Only if these efforts are unsuccessful is the FCC required to intervene. ...


"In short, while the legislation would require the Commission to address novel issues of considerable complexity, the issues relate to areas in which the Commission has historically exercised oversight responsibility."

"Network Wiretapping Capabilities," Hearing before the Subc. on Telecommunications and Finance of the House Comm. on Energy and Commerce, 103rd Cong., 2d Sess. (Sept. 13, 1994) at 80.

IV. Conclusion

The initial phase of CALEA implementation has demonstrated that if the process continues without Commission intervention, the privacy rights guaranteed by the Constitution and the statute will be in serious jeopardy. Location information is outside the mandate of CALEA. Packet switching information violates the requirement of protecting the privacy and security of information not authorized to be intercepted. We urge the Commission (1) to adopt the industry-proposed standard after deleting the location and packet switching provisions, (2) to send the issue of packet switching back to industry and law enforcement to develop a standard that suitably protects the privacy of communications not authorized to be intercepted, and (3) otherwise to reject any requests to expand the surveillance features in the standard.

Respectfully submitted,



Jerry Berman
Daniel J. Weitzner
James X. Dempsey
Alan B. Davidson
CENTER FOR DEMOCRACY AND
TECHNOLOGY
1634 I Street, N.W.
Washington, D.C. 20006
(202) 637-9800

Stanton McCandlish
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street, Suite 725
San Francisco, CA 94103-4832
(415) 436-9333

August 11, 1997

Attachment A

- two or more call identities are merged into one call identity;
- a call identity is split into two or more call identities; or
- a call identity is changed to another call identity.

Any call identity, that is mentioned as a previous call identity that is not mentioned as a resulting call identity, is considered closed and may be reassigned to other calls.

The Change message includes the following parameters:

Table 4: Change Message Parameters

Parameter	MOC	Usage
Case Identity	M	Identifies the Intercept Subject.
Access Location	C	Included to identify the location of the Access Function when the underlying data carriage does not imply that location.
Time Stamp	M	Identifies the date and time that the event was detected.
Previous Call Identities	M	Identifies the call identities previously used in previous messages. A call identity, that was previously used and not mentioned as a resulting call identity, is closed and may be reassigned to other calls.
Resulting Call Identities	M	Identifies the call identities in the resulting call. One or more call identities may be generated for the Change message which is used to correlate subsequent messages.
Resulting CCC Identity	C	Included when contents are delivered to identify the CCC(s) in the resulting call.

5.4.5 Origination

Origination message reports circuit-mode call origination attempts and number translations for the intercept subject. More than one Origination message is possible for a single call attempt when numbers are expanded or translated.

The Origination message is triggered when:

- a call or call leg originated by the intercept subject is routed toward a destination within the accessing system;
- a call or call leg originated by the intercept subject is routed toward a destination on an external public or private network;
- the destination number for a call or call leg originated by the intercept subject is translated from one set of digits to another. For example, speed number expansion or 800-number translation; or
- a call was attempted that was partially dialed or could not be completed by the accessing system.

The Origination message includes the following parameters:

Table 5: Origination Message Parameters

Parameter	MOC	Usage
Case Identity	M	Identifies the Intercept Subject.
Access Location	C	Included to identify the location of the Access Function when the underlying data carriage does not imply that location.
Time Stamp	M	Identifies the date and time that the event was detected.
Call Identity	M	Uniquely identifies a call within a system. A unique call identity may be generated for the Origination message which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call (e.g., three-way calling or conference calling for some systems).
Calling Party Identity	C	Include when more specific than the intercept subject identity associated with the case identity to identify the originating number.
Called Party Identity	C	Include when known to identify the called party. This shall not be present for calls that were partially dialed or could not be completed by the access system.
Input		Include when specific user or translation input is known. This may be present without information if a call is attempted without input (e.g., hot line).
Location		Include when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
Transit Carrier Identity	C	Include when the transit network selection is known to identify it.
Bearer Capability	C	Include when known (or presumed) to indicate the requested bearer service for the origination.

5.4.6 PacketEnvelope

The PacketEnvelope message is used to convey data packets over the CDC as they are intercepted. (Packet-mode communications delivered over CCCs or packet-mode communications using circuit-mode facilities do not use the PacketEnvelope.)

The PacketEnvelope message may be triggered when:

- a packet-mode user communication intended for the intercept subject is detected; or
- a packet-mode user communication from the intercept subject is detected.

The Redirection message includes the following parameters:

Table 7: Redirection Message Parameters

Parameter	MOC	Usage
Case Identity	M	Identifies the Intercept Subject.
Access Location	C	Included to identify the location of the Access Function when the underlying data carriage does not imply that location.
Time Stamp	M	Identifies the date and time that the event was detected.
Call Identity	M	Uniquely identifies a call within a system.
Redirected-to Party Identity	M	Identifies the redirected-to party.
Transit Carrier Identity	C	Included when the transit network selection is known to identify it.
Bearer Capability	C	Included when known (or presumed) to indicate the requested bearer service for the origination.

5.4.8 Release

The Release message reports the release of the resources used for a circuit-mode call.

The Release message is triggered when:

- a circuit-mode call attempt is abandoned by the calling party; or
- a completed circuit-mode call is released.

The Release message includes the following parameters:

Table 8: Release Message Parameters

Parameter	MOC	Usage
Case Identity	M	Identifies the Intercept Subject.
Access Location	C	Included to identify the location of the Access Function when the underlying data carriage does not imply that location.
Time Stamp	M	Identifies the date and time that the event was detected.
Call Identity	M	Uniquely identifies a call within a system. The Call Identity is released (except for possible use by a CCClose message).
Location	C	Include when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of an intercept subject's mobile terminal.
System Identity	C	Include when a handed-off wireless call is released to another TSP, to identify the last known TSP serving the subject.

Attachment B

The CIAP accesses a call redirected by the intercept subject. Redirection may include any rerouting of a call, for example, call delivery, call forwarding, call deflection, or call diversion. This access is independent of the intercept subject, as the intercept subject may engage in another communication or service at any time while a redirected call is in progress as shown in the following figure.

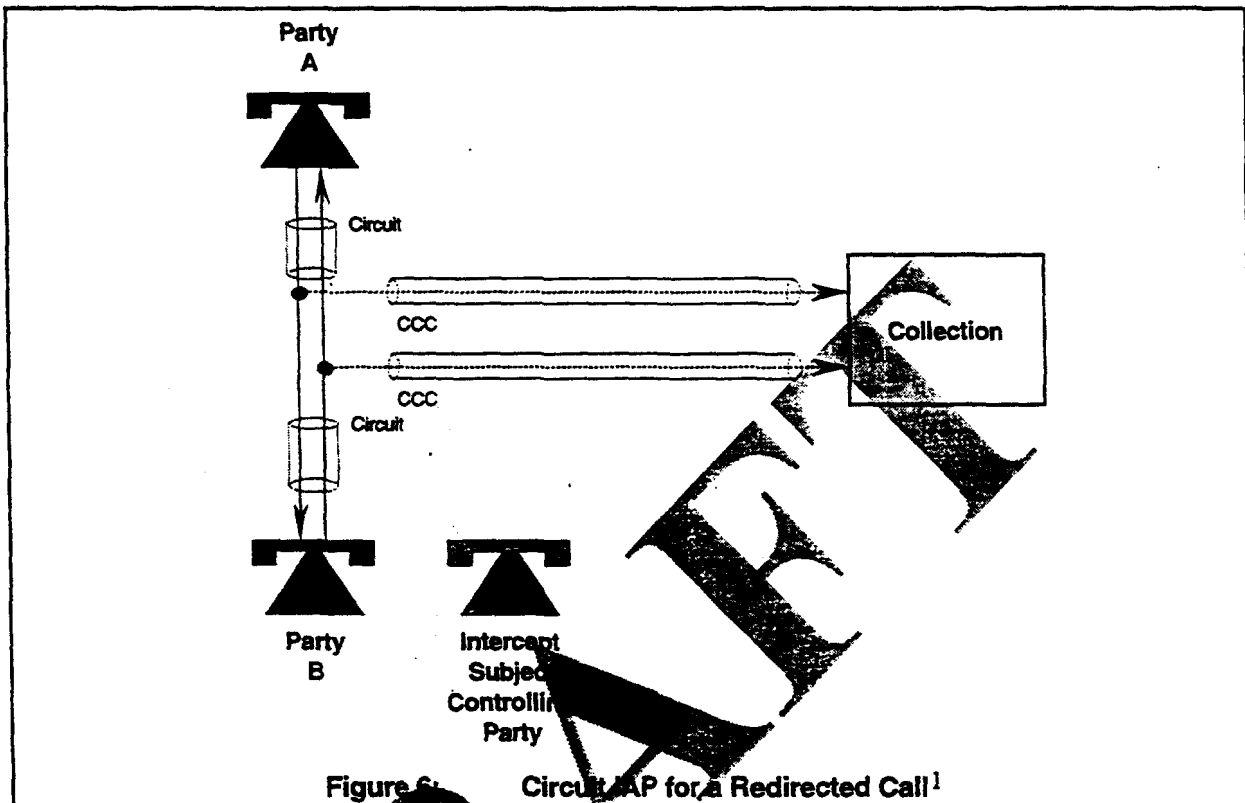


Figure 6: Circuit IAP for a Redirected Call¹

4.5.2 Packet Data IAP

Packet Data IAP (PDIAP) provides access to data packets sent or received by the equipment, facilities, or services of an intercept subject when a packet-mode data service is provided. PDIAPs may be on the Serving System or on the Redirecting System. An IAP on the Redirecting System may access only some packets delivered to the intercept subject (and possibly none of the packets originated by the intercept subject).

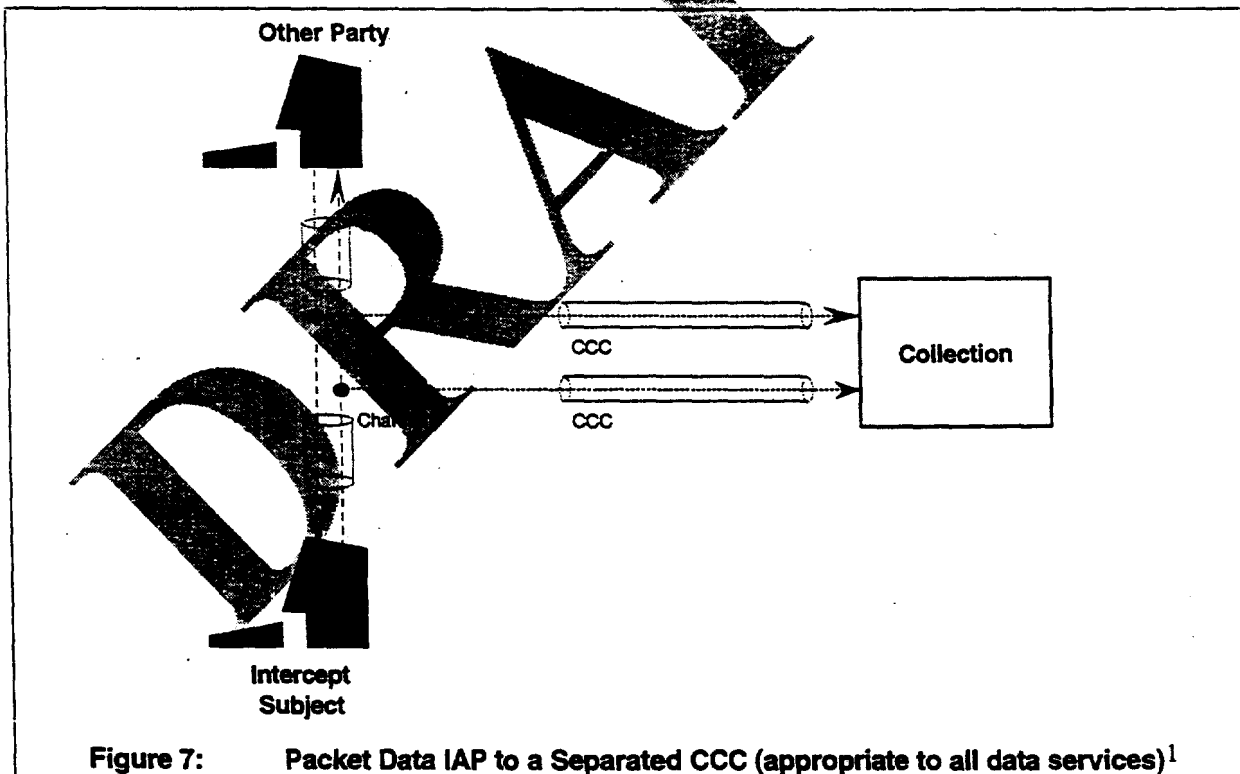
The access includes all packet-mode data transmissions regardless of their outcome. For example, when an SMS packet to a Mobile Station (MS) is intercepted, it is not known whether the packet was actually received by the MS. Packets should be sent to the Collection Function as they are intercepted.

¹ The symbols used in the figure represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

A Packet Data IAP (PDIAP) provides access to one or more of the following packet-mode data services:

- ISDN user-to-user signaling,
- ISDN D-channel X.25 packet services,
- Short Message Services (SMS) for cellular and Personal Communication Services (e.g., NAMPS, IS-41, PCS1900, or GSM-based),
- wireless packet-mode data services (e.g., Cellular Digital Packet Data (CDPD), CDMA, TDMA, PCS1900, or GSM-based packet-mode data services),
- X.25 services,
- TCP/IP services,
- paging (one-way or two-way), and
- packet-mode data services using traffic channels.

CCCs may be used to transport packet data to the Collection Function as shown in the following figure. The intercepted packets shall be delivered without interpretation or modification, except for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function.



¹The symbols used in the figure represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.

Connectionless data services may use separated delivery as shown above or they may use combined delivery as depicted in the following figure.

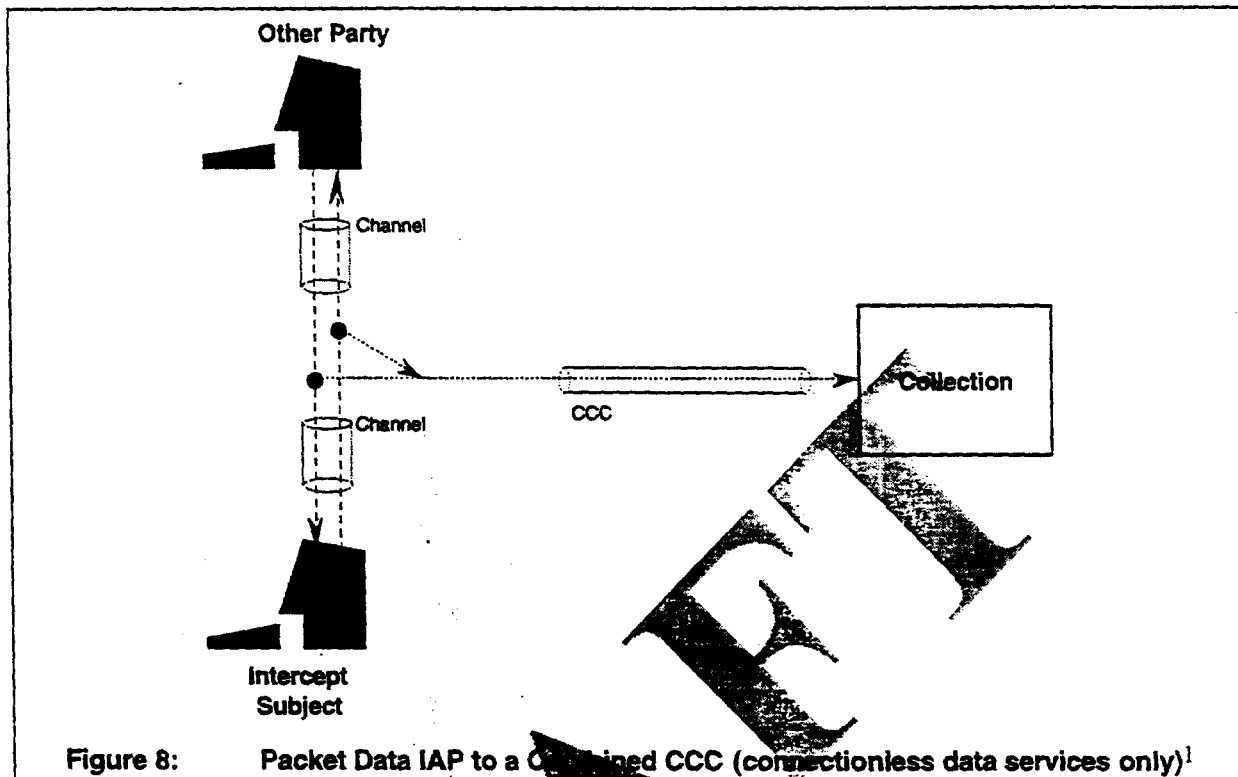


Figure 8: Packet Data IAP to a Combined CCC (connectionless data services only)¹

¹ The symbols used in the figure represent generic telecommunication terminals and services. The symbols should not be taken to exclude any particular technology.